oswald

HEALTH CARE REFORM ADVISORY

HHS Guidance on Audio-Only Telehealth & Reproductive Care Privacy

The Department of Health and Human Services (HHS) has recently issued several new pieces of guidance related to compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Clinical and Economic Health Act of 2009 (HITECH).
This advisory will provide a high-level summary of each of these guidance pieces and what they mean for employer-sponsored group health plans.

HIPAA Compliance Requirements for Audio-Only Telehealth
In June, HHS issued guidance on how providers and health plans can remain in compliance with HIPAA's privacy, security, and breach notification rules when offering audio-only telehealth benefits. Many providers and health plans offer telehealth services. For the duration of the COVID-19 public health emergency, the Office of Civil Rights (OCR, the enforcement division of HHS) has indicated that it will exercise its enforcement discretion and will not impose penalties for noncompliance with the requirements of the HIPAA Rules in connection with the good faith provision of telehealth using non-public facing audio or video remote communication technologies. However, once the emergency ends, it will be important for covered entities to ensure they are following applicable requirements.

The guidance clarifies that while audio-only services are a permissible method of providing care, covered entities must pay attention to certain requirements. The guidance is geared towards health care providers; however, employer plan sponsors will also want to pay attention with respect to any telecommunication services used as part of the health plan, and whether application of HIPAA's security rules and/or a Business Associate Agreement (BAA) may be necessary with respect to such service providers.

- First, guidance clarifies that health plans must implement reasonable safeguards, including appropriate verification procedures, to protect the privacy of protected health information (PHI) from impermissible uses and disclosures.
- In addition, the HIPAA security rules for electronic protected health information (ePHI) apply when the technology being used is anything other than a traditional land-line – e.g., voice-over-internet-protocols (VoIPs) and mobile technologies that use internet, cellular, and/or Wi-Fi, such as communication applications, electronic transcription services, and message storage services. For these technologies, covered entities must conduct a security risk analysis and ensure that appropriate security controls are applied to protect the confidentiality of the ePHI being transmitted.
- When an audio telehealth application/provider is acting as more than a conduit for ePHI, a BAA is necessary. For example, a smartphone app offered by a health care provider that stores ePHI (*e.g.,* recordings, transcripts) in the app developer's cloud infrastructure for later use. In this case, the app would not be providing mere data transmission services and would instead also be creating, receiving, and maintaining ePHI. Because it is not merely a conduit for transmission of the ePHI, a BAA with the app developer would be required. For this purpose, plans should consider whether an application or provider is "creating, receiving, or maintaining ePHI" on the plan's behalf or whether it needs access on a routine basis to the PHI it transmits in the call. If it is and/or does, then a BAA is needed.

This guidance may be found HERE.

Post-Dobbs Guidance for Reproductive Health Privacy

In a separate piece of guidance, HHS outlined the ways in which existing privacy regulations protect the confidentiality of information related to reproductive health services, and also addressed the scenarios in which disclosures of PHI by providers or health plans would and would not be permissible. The guidance focuses primarily on certain exceptions under the privacy regulation to the general rule that PHI may only be used and disclosed without written authorization if it is for purposes of "treatment, payment and health care operations." Such exceptions include incidents like disclosures that are required by law; disclosures to law enforcement; and disclosures made to avert a serious threat to health and safety.

1. Disclosures Required by Law. HIPAA permits certain disclosures of PHI when the disclosure is required by a law that is enforceable in a court of law, as long as the disclosure complies with the requirements of the law. This exception to disclose PHI as "required by law" is limited to "a mandate contained in law that compels an entity to make a use or disclosure of PHI and that is enforceable in a court of law." The guidance highlights the fact that when a law does not contain a specific reporting requirement, a covered entity would not be able to make a disclosure of PHI under this exception.
2. Disclosures for Law Enforcement Purposes. This exception permits disclosures for law enforcement purposes "pursuant to process and as otherwise required by law" such as court orders, subpoenas and summons, and warrants.
3. Disclosures to Avert a Serious Threat to Health or Safety. The Privacy Rule permits (but does not require) a covered entity, consistent with applicable law and standards of ethical conduct, to disclose PHI if the covered entity, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and the disclosure is to a person or persons who are reasonably able to prevent or lessen the threat.

The guidance, which clarifies how these exceptions work and provides examples of what would or would not constitute a permissible disclosure under each exception, is primarily aimed at providers. However, there could be implications for employer-sponsored group health plans as well. First, the guidance is a reminder to plan sponsors that there are specific rules about if, when, and how PHI may be used or disclosed. Violation of these requirements may be considered a reportable breach. Second, employer plans that cover reproductive health service, including travel benefits for employees to access reproductive care, may have claims records that law enforcement or state officials may attempt to request in the future. If such benefits are offered as part of a health plan subject to HIPAA, then it will be very important to understand the circumstances under which any PHI may permissibly be disclosed to an inquiring third party without written authorization from the individual. Employers should review existing policies and procedures and practices to ensure there are compliant processes in place with respect to how PHI is used and disclosed by the plan.

This guidance may be found HERE.

Oswald Companies | Health Care Reform Implementation
Danielle Jarvis, Compliance Team Leader | djarvis@oswaldcompanies.com; 216.649.7384
Group Benefits Compliance gbcompliance@oswaldcompanies.com